



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,500	03/26/2004	Masakazu Nishida	9683/175	8158
27879	7590	07/20/2009	EXAMINER	
INDIANAPOLIS OFFICE 27879 BRINKS HOFER GILSON & LIONE CAPITAL CENTER, SUITE 1100 201 NORTH ILLINOIS STREET INDIANAPOLIS, IN 46204-4220				ROSE, KERRI M
ART UNIT		PAPER NUMBER		
2416				
			MAIL DATE	DELIVERY MODE
			07/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/810,500	NISHIDA ET AL.	
	Examiner	Art Unit	
	KERRI M. ROSE	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 21 May 2009.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 6-18 and 26-32 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 6-18 and 26-32 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

- Certified copies of the priority documents have been received.
- Certified copies of the priority documents have been received in Application No. _____.
- Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) Notice of Informal Patent Application

6) Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/21/2009 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 6-18 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 9 recites the limitation "the user interface" in the fourth line. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 6-18 and 26-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Lipkin et al. (US 6,138,235), provided by applicant.

7. In regards to claim 6, Lipkin discloses a computer terminal (Fig. 1 element 140 discloses a third party system. Col. 3 lines 8-26 disclose the system can be a computer terminal.) comprising:

A memory (Fig. 1 discloses third party system, 140, downloads code modules, 112 and 122, and stores them in a memory.);

A receiver configured to communicate over a network, wherein the receiver is further configured to receive, through the network, a first program from a first network location (Fig. 1 discloses system 140 receives a first program code module and a second program code module through the network. One module is received from server 110 and the other from server 120.);

The receiver further configured to receive, through the network, a second program from a second network location (Fig. 1 discloses system 140 receives a first program code module and a second program code module through the network. One module is received from server 110 and the other from server 120.);

A processor in communication with the memory and the receiver, the processor configured to store the first program in a first portion of the memory (A processor is inherent in a computer terminal. Fig. 1 discloses storing each code module in a portion of the memory.);

The processor configured to store a first communication address in association with the first program, wherein the first communication address corresponds to the first network location from which the first program is received (Fig. 4 discloses that each code module is accompanied by certificate information, such as 404, 408, 412, and 416. The

certificate information generation is dependent upon such factors as originating server, as disclosed in fig. 4 element 400. Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard. The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.);

The processor further configured to store a second program in a second portion of the memory. (Fig. 1 discloses storing each code module in a portion of the memory.);

The processor further configured to store a second communication address in association with the second program, wherein the second communication address corresponds to the second network location from which the second program is received (Fig. 4 discloses that each code module is accompanied by certificate information, such as 404, 408, 412, and 416. The certificate information generation is dependent upon such factors as originating server, as disclosed in fig. 4 element 400. Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard. The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.);

The processor configured to store second program data in a third portion of the memory, wherein the third portion of memory is assigned to the second program (Col. 3 lines 53-56 disclose that the second program may need to access a database stored in a third portion of the memory.);

The processor further configured to execute the first program stored in the memory (Figs. 1 and 2 disclose executing the program modules.);

In response to a request from the first program executed on the processor to access the second program data stored in the memory of the computer terminal, the processor further configured to determine whether the first communication address matches the second communication address (Fig. 2 discloses a process for requesting access to a second module by a first module. Fig. 5 step 516 and col. 7 lines 25-39 disclose determining if the certificates authorize the requested access by matching certificates.); and

In response to determination that the first communication address associated with the first program matches the second communication address associated with the second program, the processor further configured to permit the first program to access the second program data associated with the second program (Fig. 1 discloses the two modules operating together. Fig. 2 step 212 and Fig. 5 step 520 disclose permitting access if authorization is provided.).

8. In regards to claim 7, Lipkin discloses the computer terminal of claim 6, further comprising:

a user interface in communication with the processor (Col. 3 lines 14-16 disclose the terminal may be a personal and/or portable computer among other embodiments. At least those two embodiments include a user interface for interacting with the user.), the user interface configured to receive a user input from a user of the computer terminal (Col. 2 line 67 discloses a user may grant permission.);

the processor further configured to generate with the user interface a request for permission for the first program to access the second program data associated with the second program (Fig. 2 “Request Ticket” and Fig. 5 step 514 is a request for permission.);

the processor is further configured to receive the user input from the user interface and determine whether the first program has permission to access the second program data associated with the second program based upon the user input (Fig. 5 step 516 determines if permission should be granted.); and

wherein the processor is configured to determine whether the first communication address matches the second communication address in response to determination that the user input indicates permission for the first program to access the second program data associated with the second program (Fig. 5 step 516 and col. 7 lines 25-39 disclose determining if the certificates authorize the requested access by matching certificates, which include communication addresses.).

9. In regards to claim 8, Lipkin discloses the computer terminal of claim 6, further comprising:

the processor further configured to determine whether the second program permits another program to access the second program data associated with the second program (Figs. 2 and 5 disclose processes for determining authorization by matching the certificates.); and

in response to determination that the second program permits another program to access the second program data associated with the second program, the processor configured to permit the first program to access the second program data associated with the second program based

upon the determination that the first communication address matches the second communication address (Col. 1 lines 48-50 and col. 3 lines 51-64 disclose permitting the two programs to interact with one another once authorization has been given.).

10. In regards to claim 9, Lipkin discloses the computer terminal of claim 8, wherein in response to determination that the second program prohibits another program to access the second program data associated with the second program, the processor configured to generate with the user interface an indication that the second program prohibits the first program to access the second program data associated with the second program (Fig. 5 discloses a process for determining if one program may access another program and granting such access if allowed. If access is not allowed then an indication must be given. If an indication is not given then the user will not know why the attempt has failed and how to fix the problem. Additionally, without an indication the user may think his terminal is broken because the expected results are not occurring.).

11. In regards to claim 10, Lipkin discloses the computer terminal of claim 8, further comprising:

a user interface in communication with the processor (Col. 3 lines 14-16 disclose the terminal may be a personal and/or portable computer among other embodiments. At least those two embodiments include a user interface for interacting with the user.), wherein the user interface is configured to receive permission for the first program to access the second program data associated with the second program (Col. 2 line 67 discloses a user may grant permission.).

12. In regards to claim 11, Lipkin discloses the computer terminal of claim 10, further comprising:

the processor further configured to store registration information for the first program and the second program based upon the received permission and the determination that the first communication address matches the second communication address (Col. 4 lines 45-50 disclose issuing a “permit” for access once authorization is determined to be valid.); and

the processor further configured to permit the first program to access the second program data associated with the second program in the future based upon the stored registration information (Col. 4 lines 55-60 disclose retaining the permit to allow for future access.).

13. In regards to claim 12, Lipkin discloses the computer terminal of claim 6, wherein the first communication address is a first uniform resource locator and the second communication address is a second uniform resource locator (Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard. The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.).

14. In regards to claim 13, Lipkin discloses the computer terminal of claim 6, wherein the first program is associated with a first portion of the memory allocated to execution of the first program (Fig. 1 discloses the first program module is stored in its own portion of memory.);

the second program is associated with a second portion of the memory allocated to execution of the second program and wherein the second program data of the second program resides in the second portion of the memory (Fig. 1 discloses the second program module is stored in its own portion of memory.); and

wherein the processor is further configured to access the second portion of the memory to permit the first program to access the second program data associated with the second program based upon determination that the first communication address matches the second communication address (Figs. 2 and 5 disclose processes for determining authorization by matching the certificates. Col. 1 lines 48-50 and col. 3 lines 51-64 disclose permitting the two programs to interact with one another once authorization has been given.).

15. In regards to claim 14, Lipkin discloses a method for sharing data between two programs executed on a mobile terminal, the method comprising:

A memory (Fig. 1 discloses third party system, 140, downloads code modules, 112 and 122, and stores them in a memory.);

A processor storing a first program in a first portion of a mobile terminal memory of the mobile terminal (A processor is inherent in a computer terminal. Fig. 1 discloses storing each code module in a portion of the memory. Col. 3 line 15 disclose each computer node can be a portable computer.);

The processor storing, in the mobile terminal memory a first provider identifier of the first program in association with the first program stored in the mobile terminal memory (Fig. 4 discloses that each code module is accompanied by certificate information, such as 404, 408, 412, and 416. The certificate information generation is dependent upon such factors as originating server, as disclosed in fig. 4 element 400. Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard. The

X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.

The processor storing a second program in a second portion of the mobile terminal memory. (Fig. 1 discloses storing each code module in a portion of the memory.);

The processor storing in the mobile terminal memory a second provider identifier of the second program in association with the second program (Fig. 4 discloses that each code module is accompanied by certificate information, such as 404, 408, 412, and 416. The certificate information generation is dependent upon such factors as originating server, as disclosed in fig. 4 element 400. Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard. The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.);

The processor storing second program data in a third portion of the mobile terminal memory wherein the third portion of the mobile terminal memory is reserved by the processor for the second program (Col. 3 lines 53-56 disclose that the second program may need to access a database stored in a third portion of the memory.);

The processor executing the first program (Figs. 1 and 2 disclose executing the program modules.), wherein the first program is executable on the processor to request access to the second program data stored in the third portion of the mobile terminal memory reserved for the second program (Col. 3 lines 51-64 disclose that the first

program module may access data stored in a third portion of memory for the second program module.);

In response to a request from the first program to access the second program data stored in the third portion of the mobile terminal memory the processor determining whether the first provider identifier of the first program matches the second provider identifier associated with the second program (Fig. 2 discloses a process for requesting access to a second module by a first module. Fig. 5 step 516 and col. 7 lines 25-39 disclose determining if the certificates authorize the requested access.); and

In response to the determination of whether the first provider identifier matches the second provider identifier, the processor selecting to provide the second program data to the first program based upon determination that the first provider identifier matches the second provider identifier (Fig. 1 discloses the two modules operating together. Fig. 2 step 212 and Fig. 5 step 520 disclose permitting access if authorization is provided.), and to reject the request of the first program to access the second program data based upon determination that the first provider identifier mismatches the second provider identifier (Fig. 2 step 212 and fig. 5 step 520 disclose permitting access if authorization matches and therefore also disclose rejecting access if authorization does not match.).

16. In regards to claim 15, Lipkin discloses the method of claim 14, wherein the first provider identifier includes a first network address and the second provider identifier includes a second network address (Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard.

The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.).

17. In regards to claim 16, Lipkin discloses the method of claim 14, wherein the first provider identifier is a first uniform resource locator and the second provider identifier is a second uniform resource locator (Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard. The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.).

18. In regards to claim 17, Lipkin disclose the method of claim 14, wherein the processor determining whether the first provider identifier of the first program matches the second provider identifier associated with the second program further comprises:

The processor determining whether the second program permits access to the second program data stored in the third portion of the mobile terminal memory reserved for the second program (Fig. 5 step 502 determines if the program has permission for the selected set of services.); and

In response to determination that the second program fails to permit access to the second program data denying permission for the first program to access the second program data associated with the second program even if the first provider identifier of the first program matches the second provider identifier of the second program (Fig. 5 step 502 determines if permission is granted for the selected service set. If permission is granted processing continues, however if permission is not granted access will not be given even if the certificates match.).

19. In regards to claim 18, Lipkin discloses the method of claim 17 wherein in response to determination that the second program permits access to the second program data associated with the second program, comparing the first provider identifier of the first program to the second provider identifier of the second program (Fig. 5 step 504 and 506 discloses comparing the certificates after it has been determined that access may be permitted.).

20. In regards to claim 26, Lipkin discloses a computer readable media (Col. 2 lines 52-59 disclose types of computer readable media.) comprising:

A memory of a communication device (Fig. 1 discloses third party system, 140, downloads code modules, 112 and 122, and stores them in a memory.);

Computer code stored on the memory the computer code including instructions executable on a processor of the communication device (Col. 2 lines 59-66 disclose computer program modules comprised of code executable by a computer.):

Instructions to store a first program in the memory of the communication device (Fig. 1 discloses storing each code module in a portion of the memory.);

Instructions to store a first communication address in the memory of the communication device in association with the first program, wherein the first communication address corresponds to the first network location from which the first program is downloaded (Fig. 4 discloses that each code module is accompanied by certificate information, such as 404, 408, 412, and 416. The certificate information generation is dependent upon such factors as originating server, as disclosed in fig. 4 element 400. Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509

standard. The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.);

Instructions to store a second program in a second portion of the memory of the communication device (Fig. 1 discloses storing each code module in a portion of the memory.);

Instructions to store a second communication address in association with the second program, wherein the second communication address corresponds to the second network location from which the second program is downloaded to the communication device (Fig. 4 discloses that each code module is accompanied by certificate information, such as 404, 408, 412, and 416. The certificate information generation is dependent upon such factors as originating server, as disclosed in fig. 4 element 400. Col. 5 lines 12 and 13 disclose the stored certificate may include the identity of the signing authority and line 16 discloses the certificate follows the X.509 standard. The X.509 standard includes a communication address, such as the URL, under the common name, CN, field of the subject area of the certificate.);

Instructions to allocate a portion of the memory for use with the second program to store second program data (Col. 3 lines 53-56 disclose that the second program may need to access a database stored in a third portion of the memory.);

Instructions to store second program data in the portion of the memory allocated by the processor for use with the second program (Figs. 1 and 2 disclose executing the program modules. As data is produced by each program module it is stored in the memory allocated by the processor for use by the program.);

Instructions to execute the first program (Figs. 1 and 2 disclose executing the program modules.);

Instructions to in response to a request from the first program executed on the processor to access the second program data stored in the memory of the computer terminal, the processor further configured to determine whether the first communication address matches the second communication address (Fig. 2 discloses a process for requesting access to a second module by a first module. Fig. 5 step 516 and col. 7 lines 25-39 disclose determining if the certificates authorize the requested access.); and

Instructions to select to provide the second program data to the first program based upon determination that the first communication address associated with the first program matches the second communication address associated with the second program, the processor further configured to permit the first program to access the second program data associated with the second program (Fig. 1 discloses the two modules operating together. Fig. 2 step 212 and Fig. 5 step 520 disclose permitting access if authorization is provided.), and to reject the request of the first program to access the second program data based upon determination that the first communication address mismatches the second communication address (Fig. 2 step 212 and fig. 5 step 520 disclose permitting access if authorization matches and therefore also disclose rejecting access if authorization does not match.).

21. Claim 27 is rejected upon the same grounds as claim 17.
22. In regards to claim 28, Lipkin discloses the computer readable media of claim 26, further comprising:

instructions to extract the first communication address from a first application descriptive file wherein the first application descriptive file is associated with the first program (Col. 2 lines 50-52 disclose using a Java Archive file. As disclosed by applicant in fig. 2 and paragraphs 26-29 of the specification a Java Archive file is always associated with an application descriptive file and an ADF always has URL information.);

instructions to extract the second communication address from a second ADF wherein the second ADF is associated with a second program (Col. 2 lines 50-52 disclose using a Java Archive file. As disclosed by applicant in fig. 2 and paragraphs 26-29 of the specification a Java Archive file is always associated with an application descriptive file and an ADF always has URL information.).

23. Claims 29-32 are rejected upon the same grounds as claims 10, 18, 12, and 7 respectively.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KERRI M. ROSE whose telephone number is (571) 272-0542. The examiner can normally be reached on Monday through Thursday, 6 am - 3 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Aung MOE can be reached on (571) 272-7314. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kerri M Rose/
Examiner of Art Unit 2416